PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-220686**

(43)Date of publication of application : **10.08.1999**

(51)Int.Cl. **H04N 5/765**
H04N 5/781
G09C 1/00
H04L 9/32
H04N 5/225
H04N 5/232
H04N 5/915

(21)Application number : **10-035421**

(22)Date of filing : **02.02.1998**

(71)Applicant : **RICOH CO LTD**

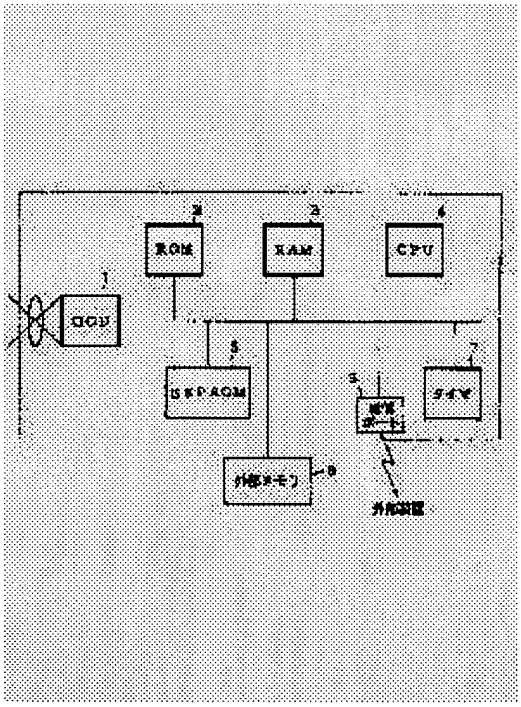
(72)Inventor : **KANAI YOICHI**
YANAIDA MASUYOSHI
NUMAZAWA MIEKO

(54) DIGITAL CAMERA

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a digital camera in which the proving strength of photographed picture data can be improved.

SOLUTION: When a shutter button is pressed, a CPU 4 obtains a time from a timer, and stores it in an RAM 3, and obtains photographic picture data from a CCD 1, and houses the data in the RAM 3, and compresses the housed picture data. Also, the CPU 4 extracts a sequence number from an EEPROM 5, and records a sequence number obtained by adding 1 to the sequence number in the EEPROM 5. The sequence number and the time data are added to the leading of the compressed picture data. A message digest using a message digest algorithm is calculated for the prepared picture information. A secret key is read from the EEPROM 5, and the message digest is enciphered. The obtained signature is added to the tail of the previous picture information so that a group of photographic information can be obtained, and recorded in an outside memory 8.



LEGAL STATUS

[Date of request for examination]	09.06.2003
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to a security system applicable to general data security about the security of a digital camera and the image data photoed with the digital camera in the detail more.
[0002]
[Description of the Prior Art] As a technique which photos an image of evidence with a digital camera, JP,7-50827,A "the accident monitoring system using a digital electronic camera" is mentioned, for example. This raises the proof nature of image data by recording the image related information of an accident related situation correctly to the image data photoed about the accident monitoring system using the digital camera carried in an automobile, and forbidding rewriting of **** of evidence or data further. In the claim 2, there is a publication "it is characterized by enabling elimination and writing by the code setting approach of fixed conditions", and the part becomes a technique used as the nucleus which prevents destruction of evidence and an alteration of image data.
[0003]
[Problem(s) to be Solved by the Invention] However, it cannot carry out by there being no indication of the concrete technique about the above-mentioned code setup or an approach in the example of above-mentioned JP,7-50827,A. Moreover, it is very difficult conventionally for a coma in a film to be serially located in a line, and for the photograph taken using the usual film to understand the order relation of the fact photoed when referring to the developed film from the photoed sequence being clear, and to forge the film moreover, to replace the photoed sequence or to change an image. However, the image data photoed with the digital camera is easy to perform an alteration, elimination, exchange of data, etc., without leaving no trace, since the data itself are digital, and the present condition is that the photoed image, i.e., the factual certification force, is low compared with what was photoed with the camera of the conventional film base.
[0004] This invention was made in consideration of the above actual condition, and is made for the purpose of offering the digital camera which heightened the certification

force of the photoed image data.
[0005]
[Means for Solving the Problem] Invention of claim 1 is held as the public key certificate which consists of a digital signature of the authentication [as opposed to / at least / a public key and this public key for the public key and private key of a pair] engine used for authentication of a public key cryptosystem, and a private key, is characterized by carrying the cryptographic algorithm of a public key cryptosystem, and the generation algorithm of a message digest, is a digital camera simple substance and adds a signature to image data.
[0006] In invention of claim 1, invention of claim 2 is characterized by enciphering inside using said private key and recording the message digest calculated inside from the image data to which said held private key had and photoed the external read-out inhibited attribute on a storage with said image data, and raises the security of a signature.
[0007] Said held public key certificate is characterized by having a rewriting inhibited attribute from the outside, and invention of claim 3 enables it to ensure verification of the signature added to image data in claim 1 or invention of 2.
[0008] Invention of claim 4 enables it to change the private key and public key certificate which are held in invention of claim 1 thru/or invention of three either, only when it is characterized by rewriting of said held private key or a public key certificate being possible when the external authentication key of at least 1 is held and the external authentication over this external authentication key is materialized and special conditions are fulfilled.
[0009] In invention of claim 1 thru/or either of 4, invention of claim 5 holds the sequence number showing the number of sheets of the photoed image, is characterized by what is recorded on a storage with the image data which photoed this sequence number, and records the sequence number of an image.
[0010] Said held sequence number is characterized by having a rewriting inhibited attribute from the outside, and invention of claim 6 prevents from changing the sequence number of an image from the outside in invention of claim 5.
[0011] Invention of claim 7 is characterized by enciphering inside using said held private key, and recording on a storage the message digest calculated inside from the image information which combined said sequence number and said image data with said image information, and prevents from separating a sequence number and image data in claim 5 or invention of 6.
[0012] in invention of claim 5 thru/or either of 7, invention of claim 8 could reset [having made and] the sequence number held, only when it was characterized by reset of said held sequence number being possible when the external authentication key of at least 1 is held and the external authentication over this external authentication key is materialized and special conditions were fulfilled.
[0013] Invention of claim 9 is characterized by enciphering inside using said held private

key, and recording on a storage the message digest calculated inside from the image information which combined the time of day which photoed image data, and this image data in invention of claim 1 thru/or either of 8 with said image information, and records a setup of the time of day managed inside in the condition that it is unseparable with image data.

[0014] A setup of the time of day managed inside is characterized by having a modification inhibited attribute from the outside, and invention of claim 10 prevents from changing from the outside a setup of the time of day managed inside in invention of claim 9.

[0015] Invention of claim 11 enables it to change a setup of the time of day managed inside in claim 9 or invention of 10, only when it is characterized by setting modification of the time of day managed inside when the external authentication key of at least 1 is held and this external authentication key is materialized being possible and special conditions are fulfilled.

[0016]

[Embodiment of the Invention] a block diagram for drawing 1 to explain one example of the digital camera by this invention -- it is -- the inside of drawing, and 1 -- CCD and 2 -- ROM and 3 -- RAM and 4 -- CPU and 5 -- EEPROM and 6 -- a communication link port and 7 -- a timer and 8 -- external memory -- it is -- cryptographic algorithm (for example, RSA and DES (Data Encryption Standard) which are shown in a U.S. Pat. No. 4405829 number.) standard to ROM2 DES may be used for external authentication. A message digest generation algorithm (for example, MD5), an image data compression algorithm (for example, JPEG), a random-number-generation algorithm, and the Maine control program are stored. The private key of a public key cryptosystem, and a public key certificate (an authentication engine's signature and public key), a sequence number and an external authentication key are stored in EEPROM5. The Maine control program, various algorithms, a private key, a sequence number, an external authentication key, etc. are loaded to RAM3 if needed. The image information which added a sequence number, time of day, a signature, etc. to the photoed image data is recorded on external memory (for example, memory card etc.) 8. In addition, an algorithm means a program here.

[0017] If a shutter release is pushed, CPU4 will acquire photography image data from CCD1, and will hold it in RAM3 at the same time it acquires time of day from a timer and memorizes it to RAM3. And the held image data is compressed. The sequence number added to the sequence number one is recorded on EEPROM5 at the same time it takes out a sequence number from EEPROM5. Next, the sequence number previously taken out at the head of the compressed image data and the time-of-day data acquired from the timer are added. And the message digest which used the message digest algorithm (for example, MD5) to the done image information is calculated. A private key is read from EEPROM5 and the message digest previously calculated using it is enciphered. And the obtained signature is added to the last of previous image information, and it considers as

the photography information on a lump, and records on external memory 8.
[0018] In case a private key, a public key certificate, a sequence number, and a time-of-day setup are changed, the following procedures perform external authentication processing which should be performed beforehand. When the algorithm used for external authentication is DES, first, a random number is generated inside and the random number is sent out to an external device. It compares with the code which enciphered the authorization code with reception from the external device, and enciphered the random number generated previously with the external authentication key. It supposes that external authentication was materialized when those codes were in agreement, and is the security status (flag managed by RAM.). An initial state is set to FALSE. It changes into TRUE.
[0019] With reference to the security status first managed inside when modification of a private key, a public key certificate, a sequence number, and a time-of-day setup is required from the exterior, when it serves as FALSE, a demand is not received. When it is TRUE, a demand is received, and processing according to the demand is performed. Processing changes the security status into FALSE.
[0020]
[Effect of the Invention] Use invention of claim 1 for authentication of a public key cryptosystem, and even if few, the public key and private key of a pair Since it held as the public key certificate which consists of an authentication engine's digital signature to a public key and this public key, and a private key and the cryptographic algorithm of a public key cryptosystem and the generation algorithm of a message digest were carried In case a signature is added to the photoed image, with required information and an algorithm, a signature can be added to image data with a digital camera simple substance, and the certification force of the photoed image data can be heightened.
[0021] Invention of claim 2 is set to invention of claim 1. Said held private key Since it enciphers inside using said private key and the message digest which has an external read-out inhibited attribute and calculated it inside from the photoed image data is recorded on a storage with said image data The reference from the outside of the private key used for generation of a signature becomes impossible. By this By being able to raise the security of a signature and adding a signature (what enciphered the message digest) to the image data which photoed the signature (what enciphered the message digest) in the photoed image The digital camera which photoed image data can be specified and the certification force of the photoed image data can be heightened.
[0022] In claim 1 or invention of 2, since said held public key certificate has a rewriting inhibited attribute from the outside, rewriting of it from the outside of a public key certificate becomes impossible, invention of claim 3 can ensure by this verification of the signature added to image data with the digital camera, can specify the digital camera which photoed image data, and can heighten the certification force of the photoed image data.

[0023] When invention of claim 4 holds the external authentication key of at least 1 in invention of claim 1 thru/or either of 3 and the external authentication over this external authentication key is materialized Since rewriting of said held private key or a public key certificate is possible Only when special conditions are fulfilled, modification of the private key held and a public key certificate is attained. By this The certification force of the image which could carry out things, renewal of a still more nearly periodical key was attained, and the security of a private key increased, and was photoed which maintains the security of a private key or a public key certificate can be heightened.
[0024] In invention of claim 1 thru/or either of 4, invention of claim 5 holds the sequence number showing the number of sheets of the photoed image, and since it records on a storage with the image data which photoed this sequence number, it can heighten the certification force about the context of the fact realized with the camera of the film base by record of the sequence number of an image.
[0025] In invention of claim 5, since said held sequence number has a rewriting inhibited attribute from the outside, modification of invention of claim 6 from the outside of the sequence number of an image becomes impossible, and thereby, it can raise the security of a sequence number and can heighten the certification force about a factual context.
[0026] Invention of claim 7 the message digest calculated inside in claim 5 or invention of 6 from the image information which combined said sequence number and said image data Since it enciphers inside using said held private key and records on a storage with said image information A message digest can be calculated by the ability to double a sequence number and image data, a signature can be created, it can be made by this what cannot separate a sequence number and image data, and the sequence number can raise the certification force about a factual context.
[0027] Since reset of said held sequence number is possible for invention of claim 8 when the external authentication key of at least 1 is held and the external authentication over this external authentication key is materialized in invention of claim 5 thru/or either of 7 By making resettable the sequence number held, only when special conditions are fulfilled By being able to maintain the security of a sequence number and resetting a sequence number still more nearly periodically It can prevent being able to manage a sequence number in the range which is useful for proving a factual context, and a sequence number's becoming large recklessly, and becoming the number which is hard to treat.
[0028] Invention of claim 9 the message digest calculated inside from the image information which combined the time of day which photoed image data, and this image data in invention of claim 1 thru/or either of 8 Since it enciphers inside using said held private key and records on a storage with said image information, it can record in the condition that the time of day managed inside is unseparable with image data, and, thereby, the certification force about the time of day when image data was photoed can be heightened.
[0029] In invention of claim 9, a setup of the time of day managed inside enables

modification from the outside of a time-of-day setup managed inside since it has a modification inhibited attribute from the outside, and can raise the security about a setup of time of day by this, and invention of claim 10 can heighten the certification force about the time of day when image data was photoed.
[0030] Since setting modification of the time of day managed inside when the external authentication key of at least 1 is held and this external authentication dark is materialized in claim 9 or invention of 10 is possible for invention of claim 11 Only when special conditions are fulfilled, modification of a time-of-day setup managed inside is enabled, thereby, maintaining the security about a setup of time of day, it can be periodically set as exact time of day, and the certification force about the time of day when image data was photoed can be heightened.

[Translation done.]